NIH Remote Access User Certification Agreement

An employee, contractor, or other authorized user is authorized by management to have remote access connectivity to NIH resources if there is a clear mission-related need.

1. All remote access connections and services that connect to NIH resources, whether furnished by the government or by the user, shall be used only by the individual authorized below and for authorized use only.
2. All authorized users who have been provided remote access to NIHnet must take annual NIH Computer Security Awareness Training at http://irtsectraining.nih.gov.
3. All new and current authorized users are required to take the NIH Securing Remote Computers course available at http://irtsectraining.nih.gov. This course provides a Certificate of Completion that can be printed and submitted to the entity granting the remote access account. Users are only required to take the course once.
4. All authorized users shall ensure that resources remain secure from damage and unauthorized use in accordance with all NIH IT security policies and procedures, including but not limited to:
    - The Limited Authorized Personal Use of NIH Information Technology Resources Policy at http://www3.od.nih.gov/oma/manualchapters/management/2806/
    - The NIH Remote Access Policy at http://www3.od.nih.gov/oma/manualchapters/management/2810/
    - The NIH Remote Access Security Standards and Procedures at http://irm.cit.nih.gov/nihsecurity/NIH_RAS_Sec_Stand_Proc.doc
    - The NIH IT General Rules of Behavior at http://irm.cit.nih.gov/security/nihitrob.html
    - The DHHS IRM Policy for IT Security for Remote Access at http://irm.cit.nih.gov/itmra/HHS-IRM-2000-0005.html
    - All IT security and remote access policies of the IC

Note: ICs may require authorized users to sign additional remote access user agreements with more stringent requirements.

5. Authorized users are also responsible for:

    - Ensuring that systems are secure and that anti-virus software is installed, running, and updated regularly on all end user remote access systems prior to using them. Authorized users of NIH-provided software should obtain the software from http://www.antivirus.nih.gov/.
    - Ensuring that, they utilize, maintain, and store highly sensitive information on NIHnet servers when feasible.
    - Reimbursing the government for any unauthorized use of government resources (by self or other individuals) or damages that result in charges to the IC that result from inappropriate use.
    - Notifying their account sponsor and supervisor when remote access resources and services are no longer required to accomplish mission objectives.

6. If authorized users require the use of remote access resources after they have left the IC, such as for collaboration with NIH staff, the users must have approval from the IC approving official.
7. NIH will review all remote access accounts (at least) annually to ensure that there is a continuing need for the remote access resources and privileges.

NIH Remote Access User Certification Agreement

Any remote access user found to have violated these standards and procedures is subject to cancellation of his or her remote access service and disciplinary action.

AUTHORIZED USER CERTIFICATION

I have read and understand the requirements stated above and agree to adhere to them for the duration of time I have NIHnet remote access services.

_____
Name of Authorized User

_____ _____
Signature of Authorized User Date

_____ _____
Signature of Approving Official Date

This form is available on the NIH IT Security web page at
http://irm.cit.nih.gov/nihsecurity/RA_User_Cert_Agreemt.doc